Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

Cloud Resource Optimization Based on E.C.C. with D.H. and Efficient Scheduling Algorithm

Akanksha Sharma
M.tech. Scholar, Dr C.V. Raman University
(Kota) Bilaspur

S.R. Tandan
Assistant Professor, Dr C.V.Raman University
(Kota) Bilaspur

***Abstract*— Cloud Computing is associate degree Internet-centric method of computing. net is representing either the medium or the platform through that cloud computing services square measure delivered and created accessible. Cloud computing has become vernacular within the space of high performance distributed computing because it provides on demand access to share resources over net. In cloud computing huge information storage is one among the nice difficult tasks in terms of the reliable storage of sensitive and quality of storage service still as security problems is additionally arises. This paper proposes privacy protective attested access management theme with best allocation technique together with information compression technique. that is safer then the other system the planned system might concentrate to the storage capability via exploitation Huffman compression methodology and applicable coming up with used for resource allocation in cloud. this technique generates the error rate that is zero.00882. this is often the minimum error rate ever planned in varied previous papers; this less error rate results in high security of the encrypted information.**

Keywords*— Securit ,Eleptical key Cryptography, Diffie-hellman, Compression Technique in cloud.

I. INTRODUCTION

Research in Cloud computing, jointly referred to as on-demand computing is receiving heap of attention from each setting like educational moreover as industrial that can be a quite Internet-based computing that has shared method resources and data to computers and various devices on demand. Existing methodology resolve the matter arises within the previous papers. There area unit several researches has been exhausted cloud computing during which some area unit worked on cloud security wherever as some worked on planning. there's another drawback specify for cloud is storage improvement. In projected methodology planning perform for resource allocation that is probabilistic based mostly dynamic allocation algorithmic rule. a lot of of the information hold on in clouds in sensitive. so Security and privacy area unit important problems in cloud setting. In one hand, the user need to attest itself before initiating any dealing, and on totally different hand, it ought to be ensured that cloud does not tamper with the information that is outsourced. ECC-DH (Elliptical curve cryptography with Diffie-Hellman) used for breakdown this problems solely documented user are often access knowledge at intervals the cloud.

The planned system addressed the matter of service request programing in cloud ADPS. we tend to introduce a cloud surroundings that is extremely secure within the manner of access management via technique of elliptical curve cryptography and for key exchanging this technique is uses diffie-hellman algorithmic rule to reinforce the protection level in cloud [11]. to reinforce the storage capability of cloud system has associate compression technique that is Huffman secret writing technique. In cloud computing allocation tasks is additionally a difficulty there ar static and dynamic allocation ways among these 2 systems is uses Probabilistic primarily based dynamic allocation algorithmic rule for allocating resource to the users. This paper address the following issues related to the cloud computing:

i. Security in cloud: Failure to substantiate applicable security protection once pattern cloud services may ultimately finish in higher costs and potential loss of business, so eliminating any of the potential edges of cloud computing.

iii. Load leveling in Cloud Computing: Load effort is one in each of major issue inside the cloud surroundings which can be achieved via applicable coming up with formula(Scheduling or allocation method).

II. PROPOSED SYSTEM

Proposed system contain Key alternative and key exchange policy by victimization diffie-hellman and ECC(Elliptical curve cryptography) therefore security issues in cloud is also resolve. For storage and cargo reconciliation Huffman and probabilistic aware dynamic allocation formula is used therefore cloud improvement is achieved..

A. Elliptical Curve Cryptography with Diffie-hellman algorithm

Security in cloud are often achieved via Elliptical Curve Cryptography with Diffie-hellman rule.

Diffie- playwright Algorithm: In Cloud computing domain, there area unit set of significant policies, that embrace issues with privacy, anonymity, security, liability and dependability. Diffie-Hellman key exchange protocol is 1st public key cryptography theme. it absolutely was projected by Witfield Diffie and Martin playwright in 1976 [2]. The Diffie-Hellman key agreement protocol was the primary sensible methodology for establishing a shared secret over associate degree unsecured line. It uses 2 keys -- one secret and alternative non-public key. This theme relies on the problem of computing power functions for prime exponents. this can be referred to as distinct index drawback (DLP).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

Steps in the algorithm

- Alice and Bob agree on a prime number p and a base g.
- Alice chooses a secret number a, and sends Bob (g^a mod p).
- Bob chooses a secret number b, and sends Alice (g^b mod p).
- Alice computes ((g^b mod p) ^{a} mod p).
- Bob computes ((g^a mod p) ^{b} mod p).
- Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

Elliptical curve cryptography: Elliptical Curve Cryptography is an approach in cloud computing that's supported public key cryptography to supply on demand computing Security to the knowledge. Different researches have focused on the fact that user generally has to access large volumes of data from the cloud in a secured manner. ECC generates keys through the properties of the elliptic curve equation rather than the normal technique of generation because the product of terribly massive prime numbers [2]. The technology is employed in conjunction with most public key coding ways, like RSA, and Diffie-Hellman. In ECC majority of public-key crypto (RSA, D-H) use either integer or polynomial arithmetic with very large polynomials. Elliptic Curve Discrete Logarithm Problem. Elliptic Curve Cryptography is defined with help of following parameters as:

$$P = (q, FR, a, b, c, G, n, h) \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

- q: the prime umber or 2m that defines curve's form.
- FR: field representation.
- a, b: the curve coefficients.
- G: the base point (Gx, Gy).
- n: the order of G. It must be big prime number.
- h: cofactor co-efficient [22].

Elliptic Curves (EC) over finite fields are used to implement public-key protocols. The Elliptic curve is defined on either prime field GF (p) or binary field GF (2n). Since arithmetic in latter field is much faster, we work in GF (2n). An elliptic curve E is defined by the simplified projective coordinates as follow:

$$Y^2Z + XYZ = X^3 + aX^2Z + bX^3 \ldots\ldots\ldots\ldots\ldots (2)$$

This public key cryptography scheme is defined over two fields: prime Galois Field, GF (p), or over binary extension Galois Field, GF (2m). In GF (p), the equation of Elliptic Curve is:

$$Y^2 \bmod p = x^3 + ax + b \bmod p \ldots\ldots\ldots\ldots\ldots (3)$$

Where:

$$4a3 + 27b2 \bmod p \neq 0 \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

with elements of GF (p) as integers between 0 and p-1. In GF (2m), the equation of Elliptic Curve is given by:

$$y2 + xy = x^2 + ax^2 + b \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

where: $b \neq 0$. Over GF (2m), rules for point addition and point doubling can be implemented [20].Elliptic Curves on R, Elliptic curves, known and studied since centuries, used by Andrew Wiles in his proof of Fermat's last theorem are algebraic curves or Weierstra curves.

$$y^2 = x^3 + ax + b$$

B. Resource Allocation algorithm used for Load Balancing in Cloud Environment

The service providers have a huge number of users, they have to deal with massive data, which are more difficult to schedule [1]. The requests from users must be scheduled efficiently, so scheduler needs to calculate a proper sequence to response those requests.

Probabilistic workload-aware dynamic resource allocation

In our work, probabilistic models are used in the decision making process, to describe, drive and analyze cloud resource elasticity The pseudo-code of the resource allocation algorithm is presented in Algorithm 1.

Algorithm 1: The Proposed resource allocation algorithm

Input: R,C,S,T

Output: QoS estimation

```
1.  S_tvm    0.2;
2.  S_tpm    0;
3.  P_st = // Physical Machine Switching time;
4.  for r in R do
5.    α_r' = [];
6.  for t in [1,T] do
7.        ω_t* = Algorithm 2(R,C,S,T, α');
8.        ω_t'   0;
9.      for r in R do
10.           ω_t'   ω_t' + ω_r,t';
11.       α_r'.append(α_r,t');
12.     Δ = S_tvm . ω_t' ;
13.     If Δ > 0 then
14.         S_tvm   max(S_tvm(1.0 – s') P_st);
15.     else
16.         S_tvm   (1.0 + s) P_st;
17.         Q   Q - Δ / ω_t'T;
18.   Return Q;
```

Algorithm 1 main loop iterates over each time t (Lines 6–17). Initially, it obtains an estimation of resource demand using Algorithm 2, described below (Line 7). Afterwards, it computes the actual resource demands (Lines 8 and 10) and updates a by appending a r,t to each list a (Line 10). Once the difference Δ between the estimated and the actual resources demand has been computed (Line 12), the algorithm adjusts the value of according to the progression of this error. Namely, if the error in t is greater than 0, S_{tvm} becomes the maximum between $(1.0 – s')S_{tvm}$, $s'>0$ and S_{tpm} (Line 14). Both s and s are constants that contain the value 0.5ns.Conversely, if it is smaller than 0, S_{tvm} is multiplied by (1.0 + s) and Q is incremented by -Δ/(w't T) (Lines 16 and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

17). Finally, after the end of the loop, Q is returned. Here S_{tvm} defines the switching time of virtual machine S_{tpm} define the switching time of physical machine. P_{st} define the switching time in physical machine.

Algorithm 2: Estimation of resource demand
Input: R C S ,time- slot t,α'
Output: Number $_t$ of resources to be allocated

1. $_t^* \leftarrow 0$;
2. for r in R do
3. $C = S_{r.t}$;
4. $\mu_r.\sigma_r^2 \leftarrow$ MLE ($\alpha_r^{'}$);
5. α_r = draw ($N(\mu_r,\sigma_r^2)$);
6. $_t^* \leftarrow$ $_t^*$ + $_c$ α_r;
7. Return $_t^*$;

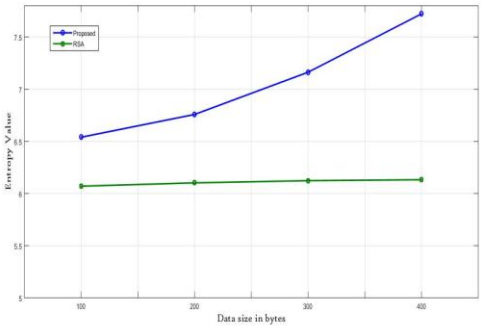
Algorithm 2 estimates the resource demand which has to be allocated to the used. Here w_t defines the resource demand by the user to be allocated.

III. EXPERIMENTAL RESULTS & ANALYSIS

The graph shows the overall performance of the system in comparison with the previous work done. The experimental results shows the workflow of the proposed methodology

Entropy Value – This value defines the security of the encrypted data .In this context, entropy is the expected average of the information contained in each message. 'Messages' can be modeled by any flow of information.

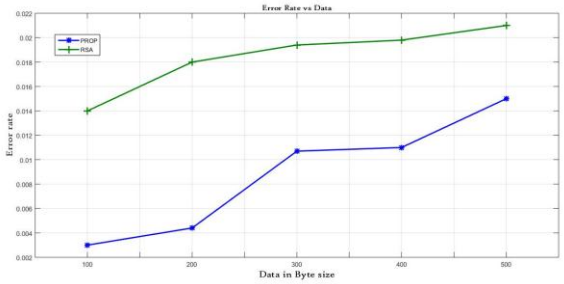
Entropy Value = -∑PI* log(PI) where PI is the data



This graph defines the relation between the data size and entropy value in which proposed value is more than the RSA. The graph concludes that RSA is lagging behind, in comparison with the proposed system which result in High Secured data.

Error Rate- Error rate of a channel. The frequency with that errors or noise square measure introduced into the channel. Error rate is also measured in terms of incorrect bits received per bits transmitted.

Error Rate = ∑ [Original – Received]^2/ Length of the original message



This graph defines the relation between data and error rate, by analyzing this graph the conclusion is that the proposed system has minimum error rate as compared with the previous system results.

IV CONCLUSION

Successful implementation of the projected system that is "Cloud Security framework supported code and compression technique and Diffie-hellman protocol". The projected technique concludes that the error rate is minimum then the previous paper. This technique consists of the protection in cloud that is handle by 2 keys that is schedule by ECC-DH that provides the entropy worth that is bigger than the opposite, which means this technique is safer than the opposite system. As per study, the previous papers didn't specialise in Storage of cloud, which might be reduced via Huffman compression technique. this technique is said to the protection problems in cloud has been victorious implement with average error rate with 2 forms of strategies for storage and resource allocation in cloud computing. within the projected system programing is finished with varied key size factors. the typical Error rate is two.94% and therefore the Average worth of Entropy worth that's shaping the protection of encrypted information is ninety three.81%.

V ACKNOWLEDGMENT

I am highly indebted to S.R. tandan Sir for his guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.
I would like to express my gratitude towards my parents & member of Dr. C.V. Raman University for their kind co-operation and encouragement which help me in completion of this project.

REFERENCES

[1] Fernando Koch, Marcos D. Assuncao, Carlos Cardoha, Macro A.S. Netto "Optimizing resource costs of Cloud computing for educatin", 2015 Elsevier.Ltd

[2] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, IEEE, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transaction and distributed system vol 25 feb 2014.

[3] Mohammad Iftekhar Husaina,n, Steven Y. Kob, Steve Uurtamob, Atri Rudrab, Ramalingam Sridharb "Bidirectional data verification for cloud storage", 2014 Elsevier.Ltd

[4] Nikos Tziritas , Samee Ullah Khana, Cheng-Zhong Xua, Thanasis Loukopoulos Spyros Lalis " On minimizing the resource consumption of cloud applications using process migrations" 2013 Elsevier.Ltd(3)

[5] Nidhi Bansala, Amitab Mauryaa, Tarun Kumara, Manzeet Singha, Shruti Bansalb "Cost performance of QoS Driven task scheduling in cloud computing" 2015 Elsevier.Ltd.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

[6] Dong Yuan∗, Yun Yang, Xiao Liu, Jinjun Chen, "On-demand minimum cost benchmarking for intermediate dataset storage in scientific cloud workflow systems", 2011 Elsevier.Ltd.

[7] Maurizio Giacobbe, Antonio Celesti, Maria Fazio∗, Massimo Villari,Q1 Antonio Puliafito "Towards energy management in Cloud federation: A survey in the perspective of future sustainable and cost-saving strategies" 2015 Elsevier.Ltd.

[8] Lifei Weia, Haojin Zhu , Zhenfu Cao , Xiaolei Dong , Weiwei Jia , Yunlu Chen, Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing" 2013 Elsevier.Ltd.

[9] Mouna Jouinia , Latifa Ben Arfa Rabaia, "Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems" 2016 Elsevier.Ltd.

[10] Rizwana Shaikha, Dr. M. Sasikumarb, "Data Classification for achieving Security in cloud computing" 2015 Elsevier.Ltd.

[11] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges" (IJCSITS) Vol. 1, No. 2, December 2011.

[12] K.Govinda , Yuvaraj Kumar, "Storage Optimization in Cloud Environment using Compression Algorithm" , IJETTCS Volume 1, Issue 1, May-June 2012.

[13] Aarti, "Performance Analysis of Huffman Coding Algorithm", Volume 3, Issue 5, May 2013 www.ijarcsse.com.

[14] Dalvir Kaur ,Kamaljeet Kaur, "Data Compression on Columnar-Database Using Hybrid Approach (Huffman and Lempel-Ziv Welch Algorithm) Dalvir", Volume 3, Issue 5, May 2013www.ijarcsse.com.

[15] Zhongyuan Lee1, Ying Wang1, Wen Zhou;"A dynamic priority scheduling algorithm on service request scheduling in cloud computing", 978-1-61284- -8/ll/$26.00 ©2011 IEEE.

[16] Xiaocheng Liu, Albert Y. Zomaya, Fellow IEEE, Chen Wang, Bing Bing Zhou, Junliang Chen, Ting Yang, : Priority-Based Consolidation of Parallel Workloads in the Cloud. IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 9, September 2013.

[17] Feng Liu, Haitao Wu, Xiaochun Lu, Xiyang Liu, Lei Fan, Genetic algorithm based optimization model for reliable data storage in cloud environment, Adv. Sci. Technol. Lett. 50 (2014) 74e79.

[18] Shachee Parikh and Richa Sinha, "Double Level Priority based Optimization Algorithm for Task Scheduling in Cloud Computing" International Journal of Computer Applications Vol. 62, No. 20, 2013

[19] Muhammad Baqer Mollah, Kazi Reazul Islam, Sikder Sunbeam Islam, "Next generation of computing through cloud computing technology", 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2012.

[20] Xiaocheng Liu, Albert Y. Zomaya, Fellow IEEE, Chen Wang, Bing Bing Zhou, Junliang Chen, Ting Yang, : Priority-Based Consolidation of Parallel Workloads in the Cloud. IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 9, September 2013.